

## **REMARKS**

Claims 1-20 are now pending in the application. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

### **REJECTION UNDER 35 U.S.C. § 112**

Claim 7 stands rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point and distinctly claim the subject matter which applicants regard as the invention. Applicant has amended Claims 6 and 7 to individually address this rejection. Applicant now believes that all pending Claims particularly point out and distinctly claim the subject matter of the present invention in combination with other elements recited in the claim. Therefore, reconsideration and withdrawal of this rejection is respectfully requested.

### **REJECTION UNDER 35 U.S.C. § 102**

Claim 11 stands rejected under 35 U.S.C. § 102(b) as being anticipated by Hirose (U.S. Pat. No. 5,917,915). This rejection is respectfully traversed.

The Examiner has cited the Hirose reference against all pending Claims, under 35 U.S.C. § 102(b). Hirose is concerned with restricting specific sections of the data to specific users and providing full access of data to other users using one master key and one secondary. Hirose decrypts a data file using one master key and one secondary key to allow specific users to view either specific portions or all of the data file. Hirose does not teach nor suggest limiting access to an encrypted data file for a specific number of times

such that the user may decrypt the data file once for each secondary key, where the decryption requires a master key and a set of secondary keys. The applicants' invention requires a master key and at least two secondary keys to decrypt a data file such that the data file may be accessed once for each secondary key in a set of secondary keys and repeating the decryption steps once for each secondary key. Accordingly, Claim 11 has been amended to recite,

Accordingly, Claim 11 has been amended to recite, "decrypting dual-encrypted blocks of the data file with the master key and at least one secondary key in a set of secondary keys, where the set of secondary keys contains at least two secondary keys, where the set of secondary keys contains at least two secondary keys." Additionally, Claim 11 has been amended to recite, "repeating the decryption steps for each secondary key in the set of secondary keys such that the device is able to access the data file content once for each secondary key in the set," where the set of secondary keys contains at least two secondary keys. Therefore, applicants believe that this claim is ready for acceptance based on the above amendment in combination with other elements recited in the claim. Thus, it is respectfully submitted that Claim 1, along with claims depending therefrom, defines patentable subject matter over Hirose. Therefore, applicants respectfully request the Examiner to reconsider and withdraw this rejection.

**REJECTION UNDER 35 U.S.C. § 103**

Claim 1 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Hirose (U.S. Pat. No. 5,917,915) in view of Watts (U.S. Pat. No. 6,587,842). This rejection is respectfully traversed.

Hirose is concerned with restricting specific sections of the data to specific users and providing full access of data to other users using a unique first key and a second key. Hirose encrypts specific types of data with the first key, then encodes all the data with a common key before transmission. The data is then decrypted using the common key which yield some news. Next, the first key is used to decrypt specific types of data where the first key is provided only to authorized users which subscribes to receive a specific/particular type of data and the common key to authorized subscribers. Hirose does not disclose the dual-encryption of a data file based on a set of secondary keys. Claim 1 recites, “generating one or more dual-encrypted blocks based on a set of secondary keys, the dual-encrypted blocks contained within the encrypted data file.” Therefore, applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Additionally, the Examiner has cited Hirose in combination with Watts in rejecting Claim 1. Hirose does not disclose, “providing the encrypted data file and an attachment file to an authorized user, the attachment file enabling a device to access the data file content once for each secondary key.” Watts is directed generally to sending an electronic message via email to a user (a product distributor) along with an attachment “binary key-file” from a second user (customer). The “binary key file” is encoded with attributes which are specific to the customer’s computer environment including a digest

which ensures the integrity of the files contents. (column 2 lines 20 – 27 and column 4 lines 35 – 47). Watts sends the “binary key file” in order to determine the integrity of the data file by comparing contents of the “binary key file” to the data file. In return, the product distributor sends a protection file to complete the installation of a computer software program.

Watts also adds that when a computer software program is downloaded that each program in the software is encoded with a key contained in a previous program downloaded to complete the installation process of the computer software. (column 2 lines 49-67; column 3 lines 5-15 ). In Watts, the downloaded program contains the key to decode the next program. Watts states that one key is used to access a single encrypted program where the programs are sent separately one after another to complete the installation of computer software not a master key and at least two secondary keys in an attached file along with an encrypted data file to allow a user access to the dual encrypted data file once per secondary key. (column 2 lines 29 – 43). Watts does not disclose sending an encrypted data file along with an attachment file containing a master key and at least two secondary keys, such that the encrypted data file can be accessed by a device once for each secondary key contained in the attachment file.

Accordingly, Claim 1 has been amended to recite “providing the encrypted data file and an attachment file to an authorized user, where the attachment file includes a master key and at least two secondary keys so that the data file can be accessed by a device once for each secondary key contained in the attachment file.” Therefore, applicants believe that this claim is ready for acceptance based on the above amendments in combination with other elements recited in the claim. Thus, it is respectfully submitted


that Claim 1, along with claims depending therefrom, defines patentable subject matter over Watts and Hirose.

#### CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: Nov. 24, 2009

By:   
Timothy D. MacIntyre  
Reg. No. 42,824

HARNESS, DICKEY & PIERCE, P.L.C.  
P.O. Box 828  
Bloomfield Hills, Michigan 48303  
(248) 641-1600

TDM/LSS/mhe